PHN 17772
LIS

Europäisches Patentamt | European Patent Office | Office européen des brevets

jc816 U.S. PTO
09/716907
11/20/00

Bescheinigung | Certificate | Attestation

Die angehefteten Unterlagen stimmen mit der ursprünglich eingereichten Fassung der auf dem nächsten Blatt bezeichneten europäischen Patentanmeldung überein.

The attached documents are exact copies of the European patent application described on the following page, as originally filed.

Les documents fixés à cette attestation sont conformes à la version initialement déposée de la demande de brevet européen spécifiée à la page suivante.

Patentanmeldung Nr. | Patent application No. | Demande de brevet n°

99203914.9

CERTIFIED COPY OF PRIORITY DOCUMENT

Der Präsident des Europäischen Patentamts:
Im Auftrag

For the President of the European Patent Office

Le Président de l'Office européen des brevets
p.o.

I.L.C. HATTEN-HECKMAN

DEN HAAG, DEN
THE HAGUE, 23/05/00
LA HAYE, LE

Europäisches Patentamt
European Patent Office
Office européen des brevets

Blatt 2 der Bescheinigung
Sheet 2 of the certificate
Page 2 de l'attestation

Anmeldung Nr.:
Application no.:
Demande n°: 99203914.9

Anmeldetag:
Date of filing:
Date de dépôt: 23/11/99

Anmelder:
Applicant(s):
Demandeur(s):
Koninklijke Philips Electronics N.V.
5621 BA Eindhoven
NETHERLANDS

Bezeichnung der Erfindung:
Title of the invention:
Titre de l'invention:
Watermark embedding and detection

In Anspruch genommene Priorität(en) / Priority(ies) claimed / Priorité(s) revendiquée(s)

Staat: State: Pays:	Tag: Date: Date:	Aktenzeichen: File no. Numéro de dépôt:

Internationale Patentklassifikation:
International Patent classification:
Classification internationale des brevets:
/

Am Anmeldetag benannte Vertragstaaten:
Contracting states designated at date of filing: AT/BE/CH/CY/DE/DK/ES/FI/FR/GB/GR/IE/IT/LI/LU/MC/NL/PT/SE
Etats contractants désignés lors du depôt:

Bemerkungen:
Remarks:
Remarques:

Watermark embedding and detection.

FIELD OF THE INVENTION

The invention relates to a method and arrangement for watermarking an information signal, for example, an audio or video signal. The invention also relates to a method and arrangement for detecting a watermark in such an information signal.

BACKGROUND OF THE INVENTION

A known method of watermarking a video signal is disclosed in International Patent Application WO-A-99/45705. In this method, a watermark pattern is added to the video signal. A watermark detector correlates the same pattern with the suspect signal. If the correlation exceeds a given threshold, the pattern is said to be present. The presence or absence of the pattern represents a single bit of information. The embedded watermark may also carry a multi-bit payload. In the system disclosed in WO-A-99/45705, the payload is represented by a combination of one or more basic patterns and spatially shifted versions thereof. The payload is encoded into the respective shift vectors. The watermark detector correlates each of the basic patterns with the suspect signal, and determines the spatial positions of the basic patterns with respect to each other. The detector further checks whether said positions constitute a valid payload.

The process of correlating watermark patterns with the suspect signal requires the watermark detector to have locally stored versions of said patterns. In view hereof, it is desired that the watermarking system employs only a few different patterns. The patterns being used are kept secret to the outside world. However, even without knowledge of the patterns, a hacker can compromise the system if he has the relevant embedder at his disposal. He may feed an arbitrary input signal to said embedder and subtract the signal from its watermarked version. The difference signal thus obtained resembles the watermark of any other watermarked signal, depending on the perception model used in the watermark embedder at hand. If the difference signal is combined with (e.g. added to or subtracted from) a watermarked signal, the embedded watermark will substantially be cancelled or at least no longer represent a valid payload. In either case, the embedded watermark has been made ineffective.

OBJECT AND SUMMARY OF THE INVENTION

It is an object of the invention to provide a more secure method and arrangement for embedding and detecting a watermark in an information signal, even if a hacker has a watermark embedder at his disposal.

To this end, the method in accordance with the invention comprises the steps of: analyzing a given property of the information signal and determining an actual value of said property; associating different watermarks with distinct values of said property; and embedding the watermark associated with said actual value. The corresponding watermark detection method comprises the steps of: analyzing a given property of the information signal and determining an actual value of said property; associating different watermarks with distinct values of said property; and detecting the watermark associated with said actual value.

With the invention is achieved that the embedded watermark pattern changes from time to time, as a function of the information signal content. Feeding an arbitrary signal to an embedder so as to produce a signal that resembles the watermark, as described above, does not work anymore because the arbitrary signal has different properties. A significant advantage of the invention is that the number of different watermark patterns that the detector must store can be held much lower. Said number is a result of balancing detector complexity versus security.

There are numerous examples of properties of the information signal that can be used for selecting the watermark pattern to be embedded. The only requirement to be fulfilled is its robustness or invariance with respect to the embedded watermark. Advantageous examples of properties are distinct distributions of luminance values of a video signal, or distinct shapes of the frequency spectrum of an audio signal.

Further aspects of the invention will be apparent from and elucidated with reference to the embodiments described hereinafter. The examples relate to watermark embedding and detection of video signals, but it will be appreciated that the invention equally applies to audio signals or any other type of multimedia signals.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 shows schematically a diagram of a watermark embedder in accordance with the invention.

Fig. 2 shows schematically a diagram of a watermark detector in accordance with the invention.

Fig. 3 shows an arrangement to illustrate the operation of the watermark embedder and detector.

Figs. 4 and 5 show further embodiments of the watermark embedder in accordance with the invention.

Fig. 6 shows a further embodiment of the watermark detector in accordance with the invention.

DESCRIPTION OF PREFERRED EMBODIMENTS

Fig. 1 shows schematically a diagram of an embodiment of a watermark embedder 1 in accordance with the invention. It will here be assumed that the embedded watermark represents a 1-bit payload. For example, the absence of a watermark indicates that the video signal may freely be copied, whereas the presence of a predetermined watermark denotes that making a copy of the signal is prohibited.

The embedder receives an input video signal I in the form of a sequence of images, and comprises an adder 11 which adds a watermark pattern W_i to each image. The embedder further comprises an image analyzer 12, a selector 13 and a read only memory 14 in which a plurality of different watermark patterns $W_1..W_N$ are stored. The analyzer 12 receives the video signal and analyzes a given property P of the video signal as function of the time. The actual value of property P found by analyzer 12 is applied to the selector 13. In response thereto, the selector selects one of the stored watermark patterns $W_1..W_N$ to the adder 11 for embedding.

The analyzer 12 may take numerous forms. A few examples will be given to provide sufficient teaching to enable a skilled person to design appropriate alternative embodiments. The property being analyzed may be the distribution of luminance values across the image (spatial distribution) or across a sequence of images (temporal distribution). In a first example, the analyzer divides each image in sub-images, and determines which of said sub-images has the highest average luminance. The relevant sub-image number is the actual value of property P. In a second example, the analyzer assigns a "0" to each sub-image having a low average luminance and a "1" to each sub-image having a high average luminance. Each video image is now characterized by an n-bit code, where n is the number of sub-images. The relevant n-bit code is the actual value of property P. The property being analyzed may also be local image activity. Such an analysis can easily be carried out in the frequency domain.

Fig. 2 shows schematically a diagram of a preferred embodiment of a watermark detector 2 in accordance with the invention. The detector receives a suspect video

signal V and comprises an image analyzer **22**, a selector **23** and a read only memory **24** that are identical to the corresponding counterparts of embedder **1**. Accordingly, the analyzer **22** analyzes the same property P of the video signal, and the selector **23** selects the same watermark pattern W from the stored patterns $W_1..W_N$, as the embedder.

The detector further comprises a correlation circuit **21** which calculates the correlation between each image of the suspect video signal and the applied watermark pattern W_i. If the correlation exceeds a predetermined threshold, the selected watermark pattern W_i is said to be present (D=1), otherwise it is said to be absent (D=0).

The correlation circuit **21** is preferably of a type which performs the correlation for all possible spatial positions of the applied watermark with respect to the image. Such a correlation circuit is disclosed in WO-A-99/45705. It generates a correlation pattern which exhibits a peak for each of the spatial positions of the watermark. In WO-A-99/45705 is described that multiple peak positions may represent a payload. However, as mentioned above, the payload in this example is a 1-bit copy control signal. The detection circuit **2** will consider the presence of 2 or more peaks as an invalid payload (D=0).

It is assumed that the watermark patterns $W_1..W_N$ are secret and can neither be retrieved by interrogating the embedder or detector circuits. As will now be explained with reference to Fig. 3, the invention prevents a hacker from compromising the system when he happens to have an embedder at his disposal. In Fig. 3, a potential hacker receives a video signal 'V' being watermarked by an embedder **1a**. The signal V' may be a recorded signal in which case the actual embedding has taken place a long time ago. The embedder **1a** is of a type as described above with reference to Fig. 1.

The hacker has a same embedder **1b** at his disposal. An arbitrary video signal X is applied to said embedder **1b** so as to locally generate a watermarked video signal X'. An adder **3** subtracts the arbitrary signal X from its watermarked version X'. The difference signal (which strongly resembles the embedded watermark pattern) is then combined with (added to or subtracted from) the watermarked signal V' by a further adder **4**. The thus processed suspect signal 'V" is applied to a watermark detector **2** as described above with reference to Fig. 2.

Without the provisions of the invention, both embedders **1a** and **1b** embed the same watermark in the respective input signals. This results either in cancellation of the watermark in the suspect signal V" or in an invalid payload due to multiple occurrences of the watermark pattern W at different positions. In both cases, the detector generates an output signal D=0 and the hacking attack is successful.

With the provisions of the invention, the watermark W_i (i=1..N) in signal V' will generally differ from the watermark W_j (j=1..N) in signal X', because the contents of the original video signals V and X are different. The property analysis algorithm of detector **2** responds to the contents of signal V" which is substantially equal to the contents of V. Consequently, the watermark pattern being checked by detector **2** is the watermark pattern W_i which has been embedded by embedder **1a**. The detector ignores the additional presence of a different pattern W_j, and the hacking attack thus fails.

A possible work-around is feeding to embedder **1b** the watermarked signal V' instead of an arbitrary signal X, so as to force embedder **1b** to select the same watermark W_i as embedder **1a**. To avoid this, the embedders **1a** and **1b** are preferably of a type that refrains from embedding a watermark in an already watermarked signal. Fig. 4 shows a schematic diagram of such an embedder. It comprises the same adder **11**, image analyzer **12**, selector **13** and ROM **14** as the embedder which is shown in Fig. 1. It further comprises the correlation circuit **21** of the detector which is shown in Fig. 2. The correlation circuit **21** detects whether the input signal I already includes the watermark pattern W_i to be embedded. If that is the case (D=1), a switch 15 is controlled to prevent the watermark pattern W_i from being embedded multiple times.

Fig. 5 shows a schematic diagram of a watermark embedder for embedding multi-bit payload in the video signal. The embedder comprises the same adder **11**, image analyzer **12**, selector **13** and ROM **14** as described before with reference to Fig. 1. The ROM **14** now stores a plurality of sets of watermark patterns. The embedder further includes an encoding circuit **16** which receives a selected set i of basic watermark patterns $W_{i,1}$, $W_{i,2}$, ..., and encodes a multi-bit payload d into the relative positions of said patterns. The basic patterns have a relatively small size (e.g. 128×128 pixels). The watermark pattern generated by encoder **16** is subsequently tiled over the image by a tiling circuit **17**. The ROM **14** stores different sets of basic patterns for different values of signal property P. The actual set of basic patterns being applied to encoder **16** is controlled by the actual value of property P and changes as a function of time.

Fig. 6 shows the corresponding watermark detector. The detector comprises a folding circuit **25** for folding and storing image segments of 128×128 pixels in a buffer prior to correlation. The detector further comprises the same correlation circuit **21**, image analyzer **22**, selector **23** and read only memory **24** as described before with reference to Fig. 2. The ROM **24** stores different sets of basic patterns for different values of signal property P. The

actual set of basic patterns being applied to the correlation circuit 21 is controlled by the actual value of property P.

It should be noted the invention is not restricted to the watermarking systems described in the embodiments. For example, a watermarking system is known that uses n different watermark patterns, each pattern corresponding to one bit of an n-bit payload. In accordance with this invention, the embedder and detector of such a system include different sets of n patterns. A particular set is then selected in response to the actual value of a signal property.

In summary, a method and arrangement for embedding and detecting a watermark in an information signal is disclosed. The embedded watermark (W_i) is selected (13) from a plurality of watermarks ($W_1..W_N$) in dependence upon a property P of the signal. An example of such a property is the distribution of luminance values of the current video image as calculated by an analysis circuit (12). The corresponding watermark detector performs the same operation: the watermark being looked for depends on the same signal property. With the invention is achieved that the embedded watermark changes from time to time as a function of the information signal content, so that it can not easily be hacked.

CLAIMS:

1. A method of embedding a watermark in an information signal, comprising the steps of:
- analyzing a given property of the information signal and determining an actual value of said property;
- associating different watermarks with distinct values of said property; and
- selecting the watermark associated with said actual value for embedding in the information signal.

2. A method as claimed in claim 1, in which the information signal is a sequence of video images, said analyzing step comprising analyzing a spatial or temporal distribution of luminance values, each distinct distribution of luminance values constituting a value of said property of the information signal.

3. A method as claimed in claim 1, in which the information signal is a sequence of audio signal segments, said analyzing step comprising analyzing a shape of the frequency spectrum of said audio segments, each distinct shape of the frequency spectrum constituting a value of said property of the information signal.

4. A method as claimed in claim 1, in which the embedded watermark is a combination of two or more basic watermark patterns constituting a set of basic watermark patterns being selected from different sets in dependence upon the actual value of the property of the information signal.

5. A method of detecting a watermark in an information signal, comprising the steps of:
- analyzing a given property of the information signal and determining an actual value of said property;
- associating different watermarks with distinct values of said property; and
- selecting and detecting the watermark associated with said actual value.

6. A method as claimed in claim 5, in which the information signal is a sequence of video images, said analyzing step comprising analyzing a spatial or temporal distribution of luminance values, each distinct distribution of luminance values constituting a value of said property of the information signal.

7. A method as claimed in claim 5, in which the information signal is a sequence of audio signal segments, the method comprising the steps of calculating the frequency spectrum for each segment, each distinct shape of said frequency spectrum constituting a value of said property of the information signal.

8. A method as claimed in claim 5, in which the embedded watermark is a combination of two or more basic watermark patterns constituting a set of basic watermark patterns being selected from different sets in dependence upon the actual value of the property of the information signal.

9. A watermark embedder for embedding a watermark in an information signal, comprising:

- means (12) for analyzing a given property (P) of the information signal and determining an actual value of said property;
- means (14) for associating different watermarks with distinct values of said property; and
- means (13) for selecting the watermark associated with said actual value for embedding (11) in the information signal.

10. A watermark detector for detecting a watermark in an information signal, comprising:

- means (22) for analyzing a given property of the information signal and determining an actual value of said property;
- means (24) for associating different watermarks with distinct values of said property; and
- means for selecting (23) and detecting (21) the watermark associated with said actual value.

11. A watermark embedder as claimed in claim 9, further including a watermark detector as claimed in claim 10, and comprising means (15) for refraining from embedding the

selected watermark in response to detection in the information signal of said selected watermark by said detector.

ABSTRACT:

A method and arrangement for embedding and detecting a watermark in an information signal is disclosed. The embedded watermark (W_i) is selected (13) from a plurality of watermarks ($W_1..W_N$) in dependence upon a property P of the signal. An example of such a property is the distribution of luminance values of the current video image as calculated by an analysis circuit (12). The corresponding watermark detector performs the same operation: the watermark being looked for depends on the same signal property. With the invention is achieved that the embedded watermark changes from time to time as a function of the information signal content, so that it can not easily be hacked.

Fig. 1

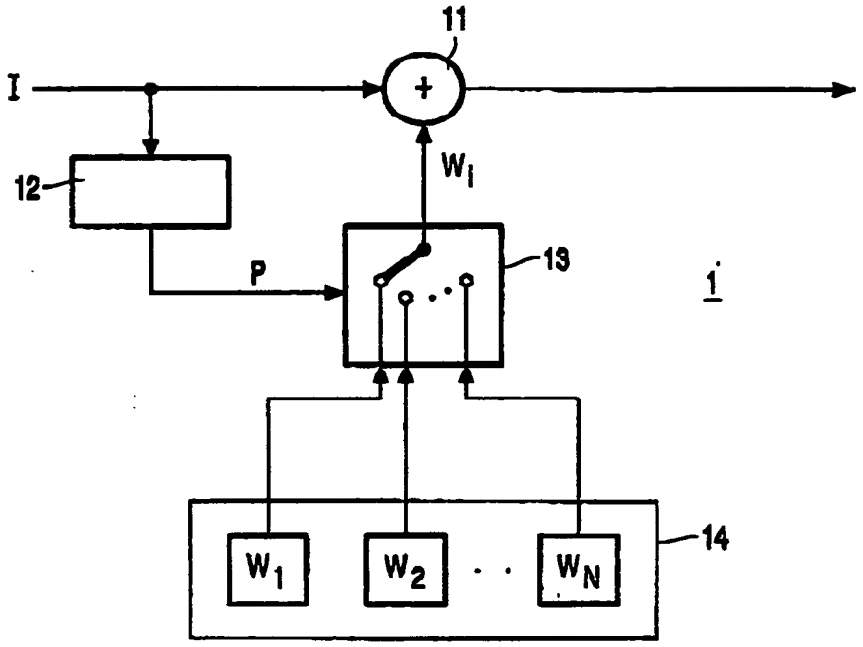

FIG. 1

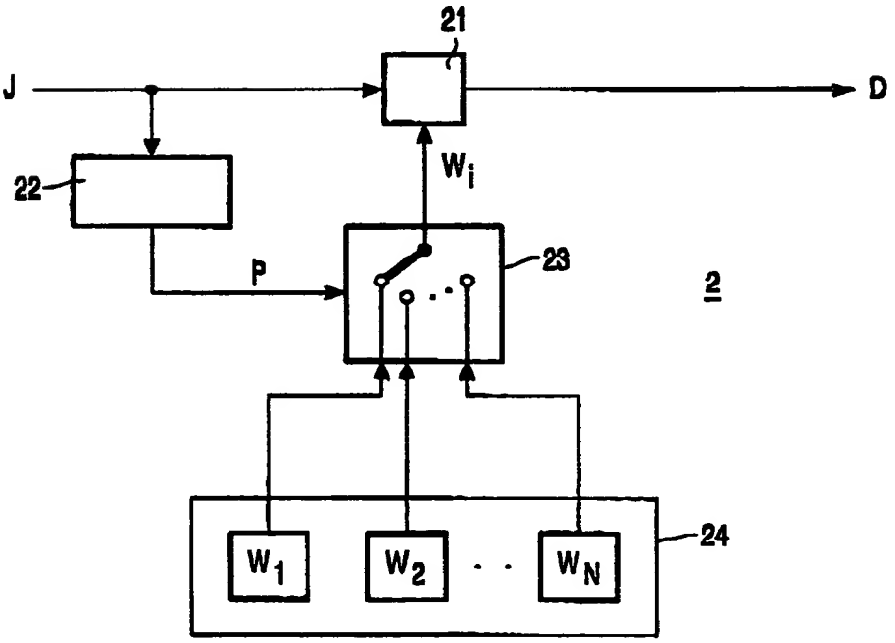

FIG. 2

2/3

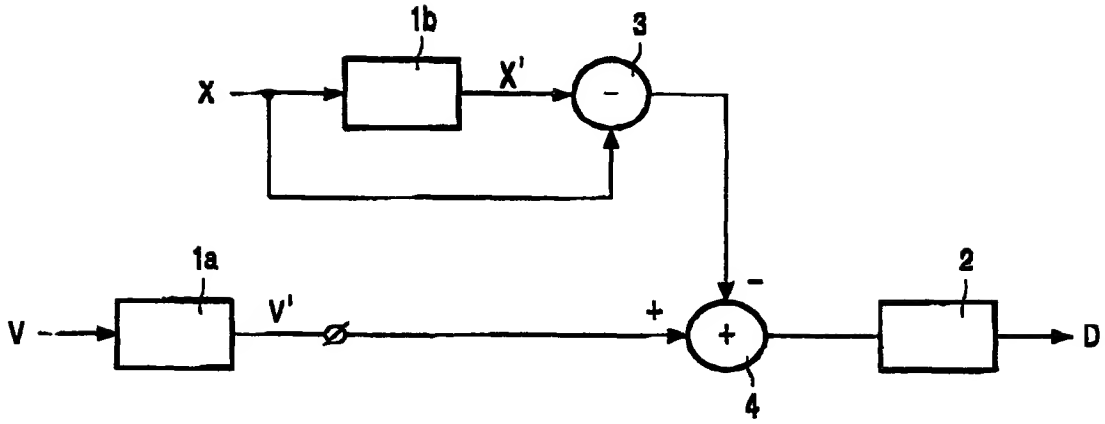

FIG. 3

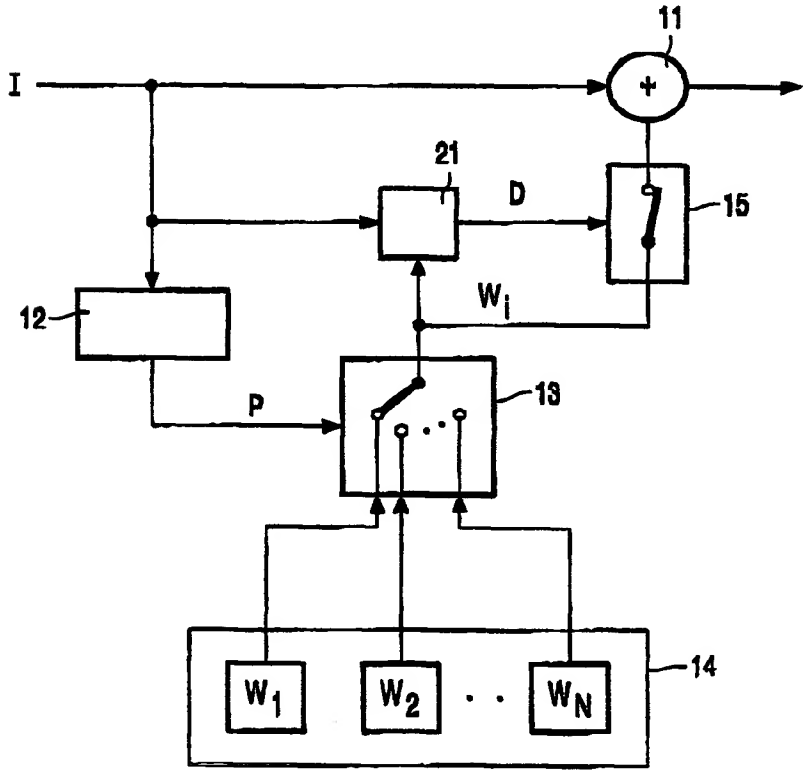

FIG. 4

2-III-PHN17772

3/3

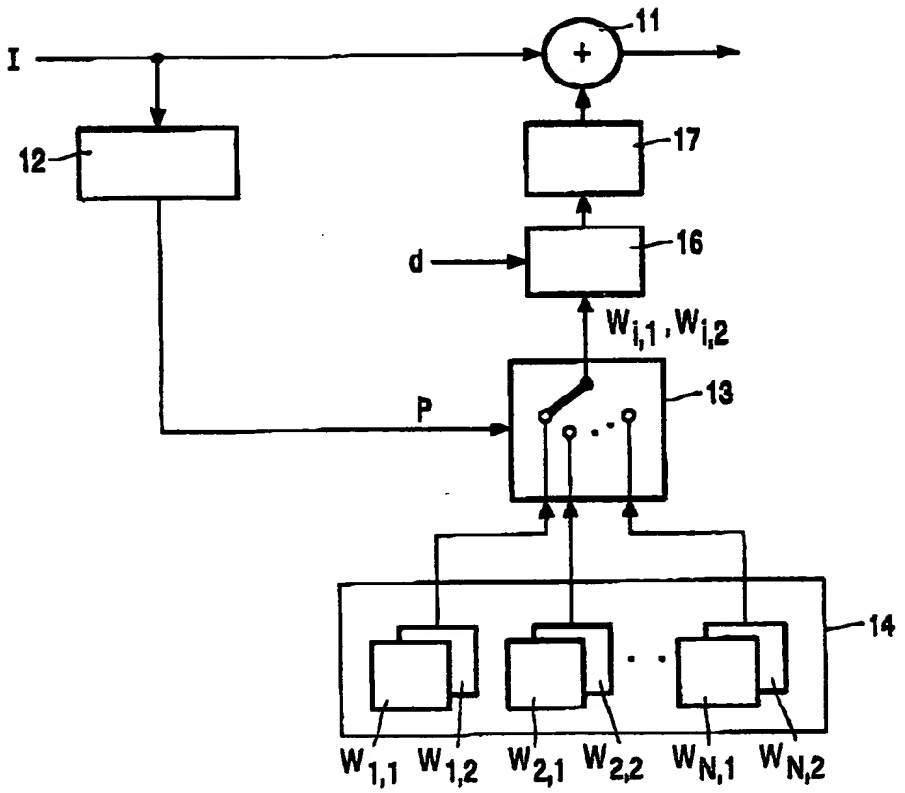

FIG. 5

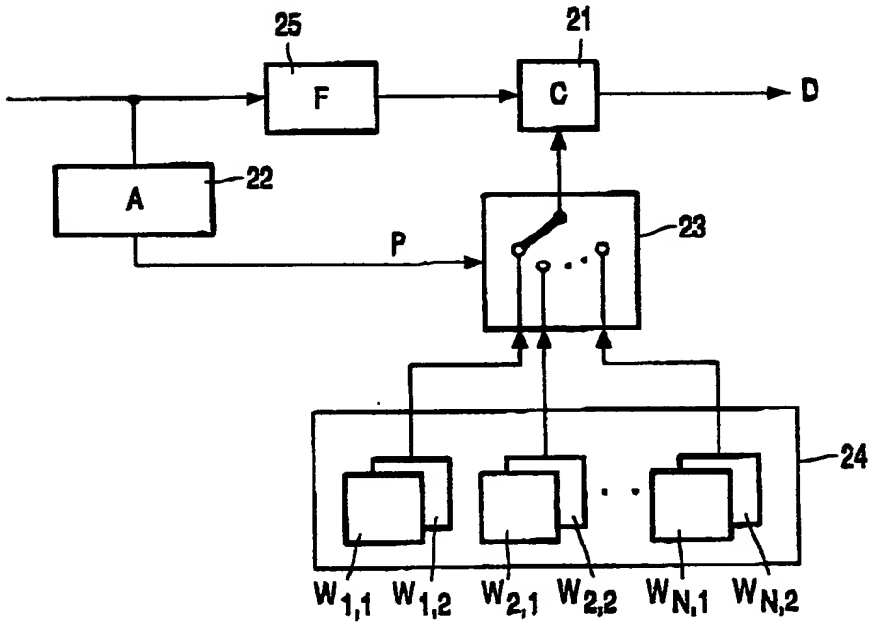

FIG. 6

3-III-PHN17772